Identity Fraud Report 2023

Onfido’s guide to preventing fraud

onfido

Contents

Foreword

By Interpol

Financial crime, fraud, and corruption are serious issues that in today's digital world, affect not only the law enforcement community but financial institutions, the private sector, and other major corporations.

The COVID-19 pandemic highlighted how quickly criminal groups and fraud rings can adapt their methods. Phone fraud, phishing, and payment card fraud are just some such examples of the tactics fraudsters used throughout the pandemic to target individuals and businesses alike.

As criminals look to take advantage of digitization processes, they're able to commit financial crimes with increasing efficiency and sophistication, to the extent that financial crime and cybercrime are now invariably linked. A significant amount of financial fraud takes place through digital technologies, and the pandemic has only hastened the emergence of digital money laundering tools and other cyber-enabled financial crimes. In a recent INTERPOL report, respondents ranked money laundering as their number one threat, with 67% putting it 'high' or 'very high' on their list.

> **This increasing interconnectivity between digitization, financial crime, and money laundering** highlights the importance of implementing robust fraud detection systems across financial institutions, governments and critical infrastructure.

Onfido, with their digital identity verification solution, are in a unique position to identify and analyze many of the fraud threats that such organizations face.

Within this report, Onfido's team of experts provides a reference guide on the emerging identity fraud trends, and outlines some of the preventative measures practitioners can put in place against them

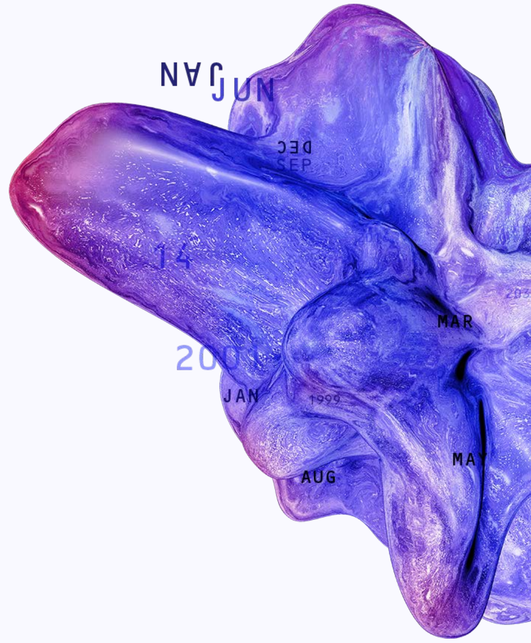
Executive summary

Fraud spikes during periods of uncertainty and instability, and the COVID-19 pandemic was no exception to this.

The years 2020 to 2021 saw all-time highs in the number of fraudulent attempts. However as the world has re-opened, the question becomes — what's next? How do businesses continue to deal with the online threats that go hand-in-hand with digitization?

Today we're seeing a unique convergence of technological advancement, online services and instantaneous digital access across the business landscape which has created a breeding ground for fraud. Increasingly, fraud is becoming a numbers game. Fraudsters are attacking at scale, favoring quantity over quality, hoping to find cracks in business defenses. Fraud is happening everywhere, 24/7, and businesses that take a reactive approach are leaving their front door wide open for fraud.

Fraudsters are attacking at scale, favoring quantity over quality, hoping to find cracks in business defenses. Fraud is happening everywhere, 24/7, and businesses that take a reactive approach are leaving their front door wide open for fraud.



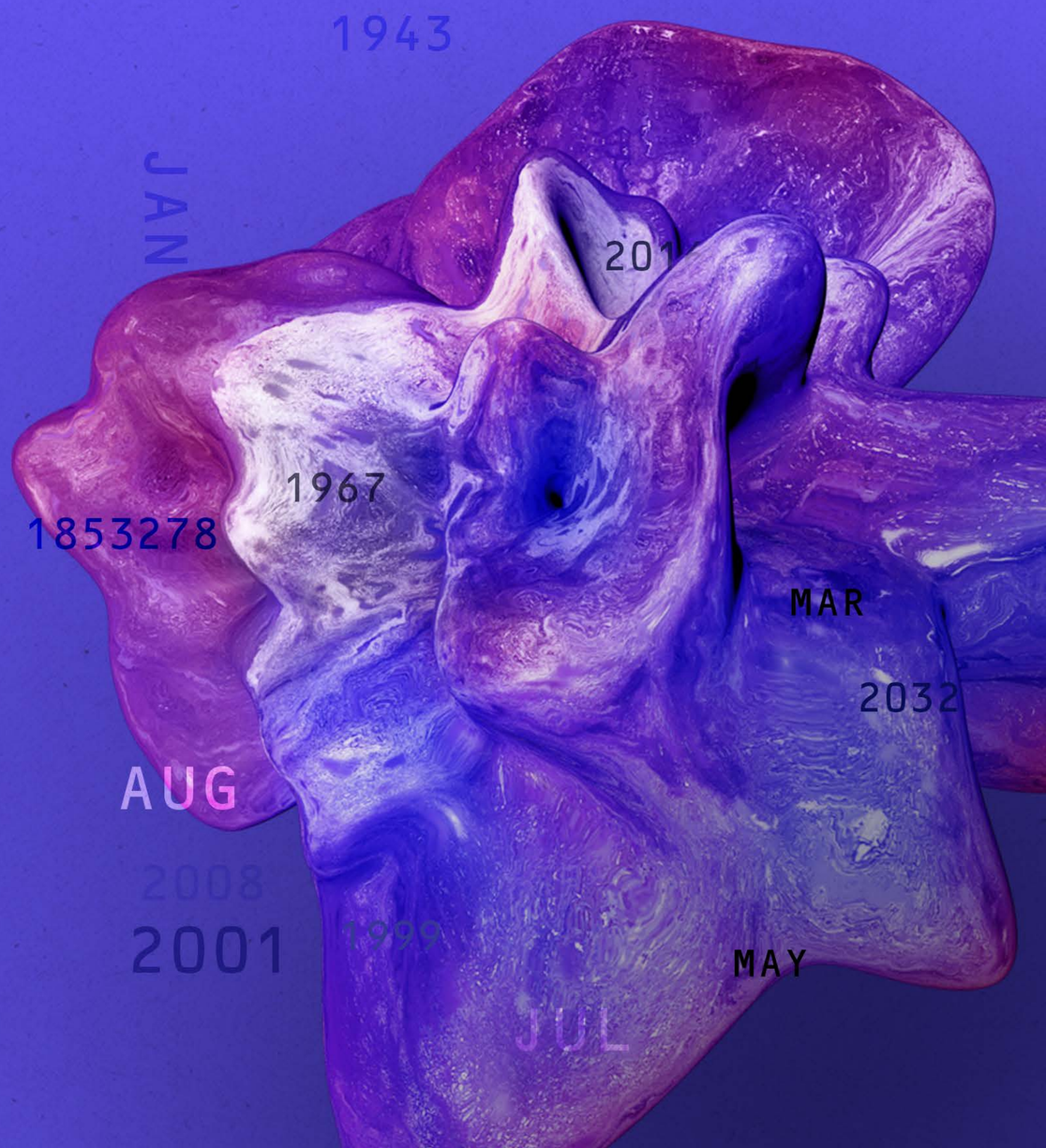
About this report

To help businesses be more proactive in their fight against fraud, this report examines how fraudsters behave, the techniques they're using, and what sort of attack patterns have emerged over the last year. From the times they're most active, to the most frequently targeted documents, to the mobile manufacturers they use most, this report dissects fraudulent activity and trends to help arm businesses for the year ahead.

Methodology

Onfido processes millions of identity verification checks every year and catches thousands of fraudulent attempts, giving us a unique insight into what methods fraudsters are adopting. The data referenced in this report was mostly taken from 1 October 2021 to 1 October 2022 and is reflective of Onfido's clients and the verification space, and therefore might not always mirror wider market trends. Onfido obtains the right to publish this data.

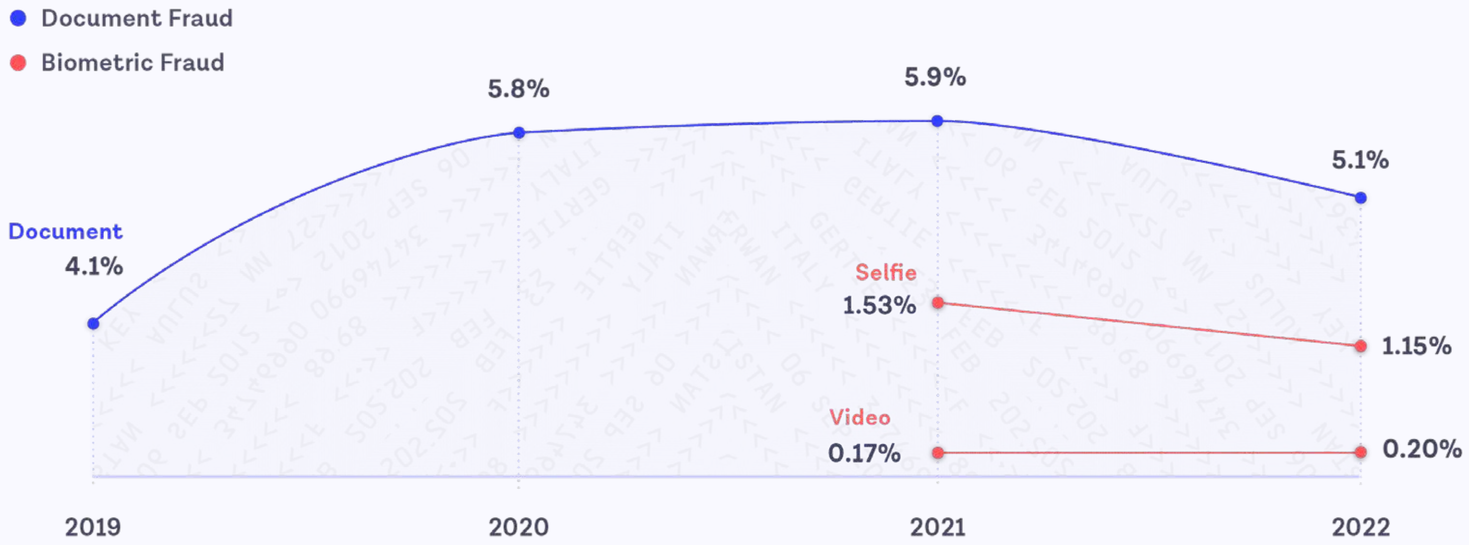
Fraud trends



Average fraud rates in 2022

The average ID fraud rate for 2022 has dropped slightly compared to what it was in 2021. From the overall trend, it's clear to see that events in 2020 and 2021 contributed to an overall spike in fraud rates:

- The COVID-19 pandemic forced many brick-and-mortar businesses to rapidly adopt digital technologies including those industries that weren't used to having to consider fraud on a daily basis. Fraudsters follow the opportunities, and as many businesses were rapidly adapting their processes for online, this opened up avenues for fraudsters to take advantage.
- Crypto also contributed to the spike in fraud rates across 2020 and 2021. In last year's report, we saw that as the price of crypto rose, so did the number of targeted attacks in that industry — soaring prices made it an attractive avenue for fraudsters. 2022 has seen a drop in crypto prices and simultaneously fraudsters' interest in this sector has declined.

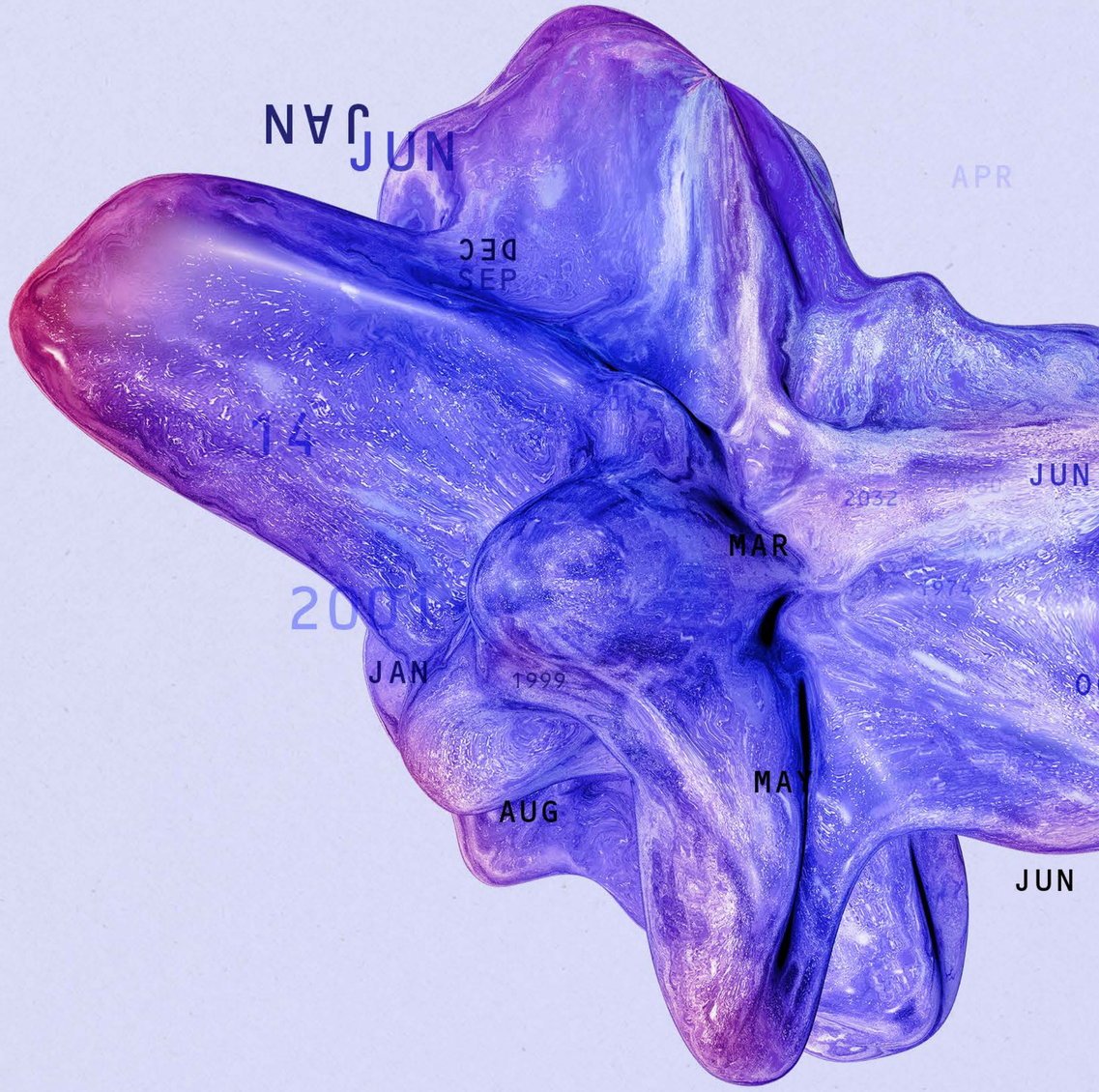


However, just because the average fraud rate has dropped doesn't mean fraud is in decline. The amount of fraud we're seeing in terms of the number of attempts is still increasing. As a business, we're processing more verifications than we were in previous years, which means the number of fraudulent attacks is rising in line with the number of verifications we process. Fraud isn't going anywhere — in fact, it's keeping pace — and businesses need to do the same.

The low average biometric fraud rates of 1.15% and 0.2% highlight the power of biometrics at deterring and detecting fraud. We will return to this point later in the report, but fraudsters generally focus their attacks on documents when attempting to bypass defenses.

The amount of fraud we’re seeing in terms of the number of attempts is still increasing.

As a business, we’re processing more verifications than we were in previous years, which means the number of fraudulent attacks is rising in line with the number of verifications we process.



Fraud is happening 24/7

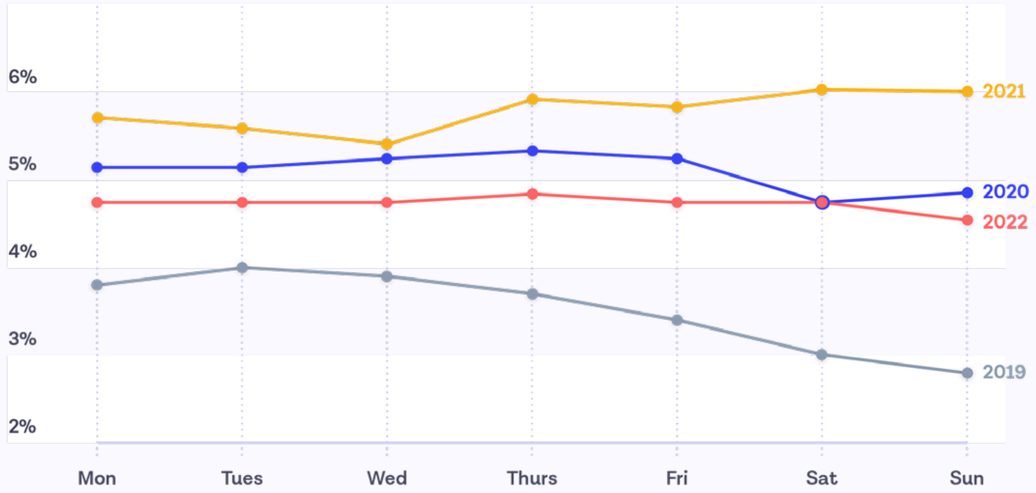
Over the last four years we've seen a shift in which days of the week fraudsters choose to launch their attacks.

Back in 2019, attacks mirrored a typical working week, peaking on Tuesdays and dropping off at weekends. Over the last three years, fraudulent activity has shifted and now we see similar levels of fraud across every day of the week. 2022 is no exception to that.

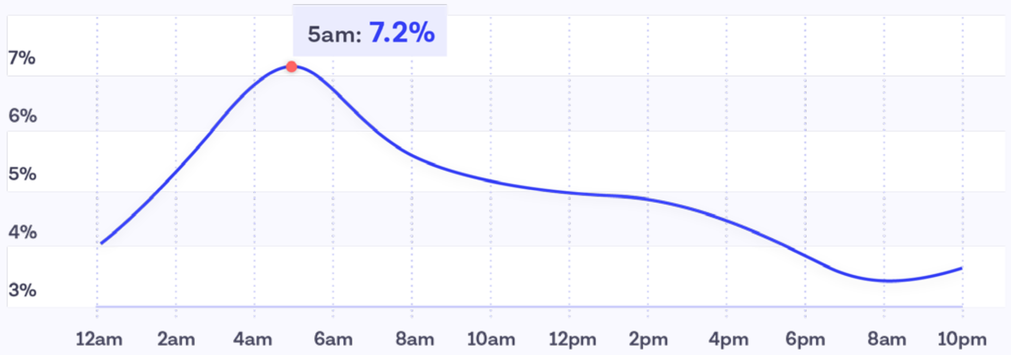
We're also seeing that fraud levels are fairly consistent across 24 hours of the day. With technology at our disposal, businesses and individuals are more connected across the globe than ever, able to traverse regions and time zones. This hyperconnectivity means there are no 'business hours' for fraudsters and sophisticated fraud rings — they will scam and defraud 24/7. Organizations need defenses that protect their business and customers every hour of every day from fraudsters across the globe.

> **Fraud is happening 24/7.** It's impossible to predict when it will happen and businesses must be prepared for attacks at any time of day, any day of the week.

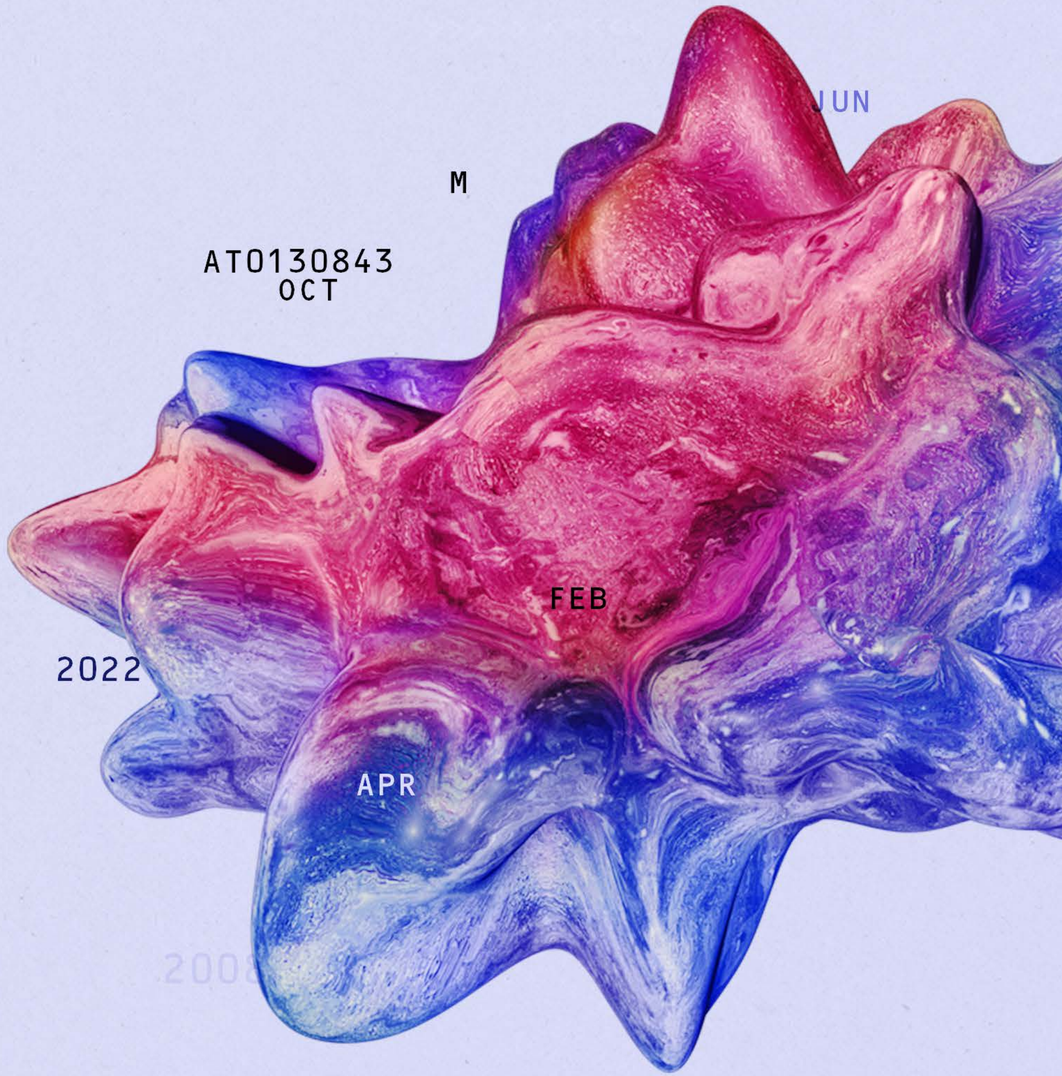
Days of the week fraudsters are most active



Time of day fraudsters are most active



With technology at our disposal, businesses and individuals are more connected across the globe than ever, able to traverse regions and time zones. **This hyperconnectivity means there are no ‘business hours’ for fraudsters and sophisticated fraud rings — they will scam and defraud 24/7.**



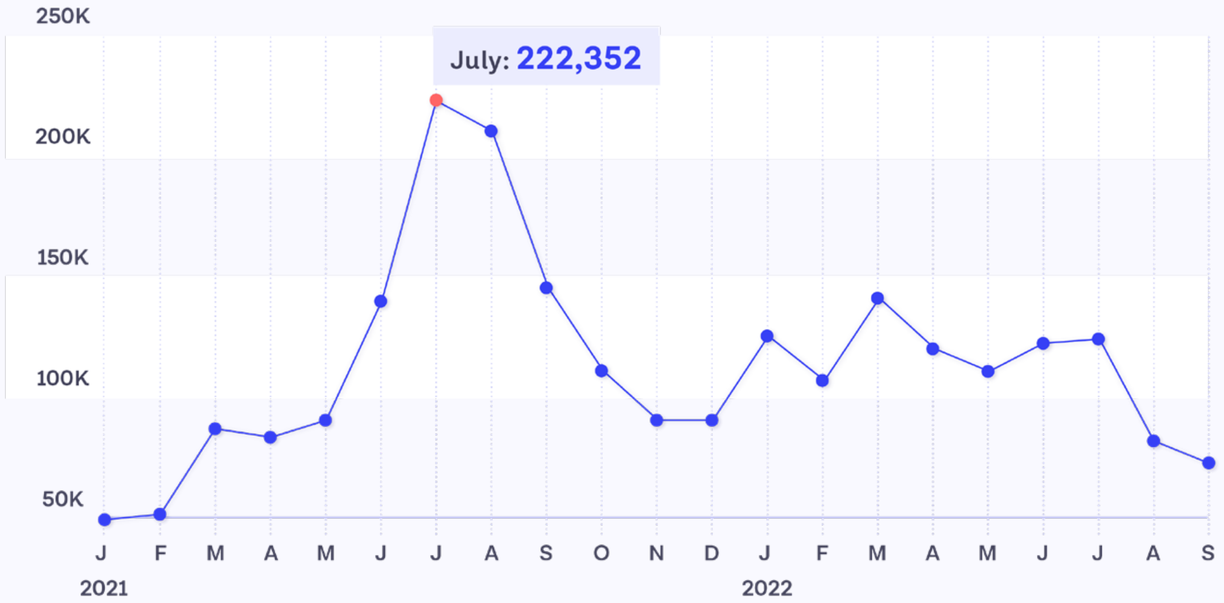
Fraud’s link to the real world

Here we examined data from the last two years to get a more accurate picture of where fraud spikes happen.

Some of the spikes will be directly related to certain client activity — but the overall trend gives a good indicator of how fraud mirrors the events of the world around it. We know that time and again fraudsters will go where there is an opportunity.

The big spike in fraud we see in July-August 2021 is around the time that much of the world began opening up again. Events like the Olympics were taking place, and businesses were once again starting to ramp up and operate ‘as normal’. It’s likely that this re-opening of business as usual is linked to a large spike in fraud. People were once again going about their day-to-day, whereas previously many were isolating or spending a lot more time at home. This explosion in activity no doubt presented many opportunities for fraudsters.

Time of year fraudsters are most active



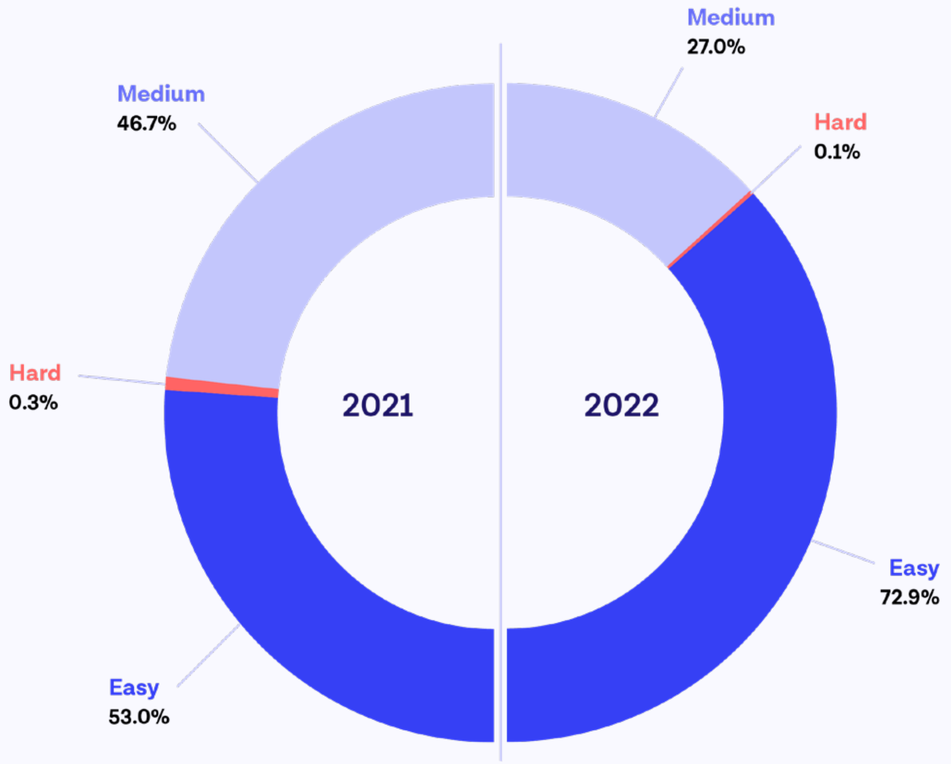
A numbers game: quantity over quality

What we classify as ‘easy’ or less sophisticated fraud has risen dramatically (37%) over the last year.

Last year, 53% of all document fraud we saw fell into this bucket, whereas this year that number has risen to 72.9%. While this might sound like good news, it simply highlights that fraud is becoming a matter of quantity over quality as fraudsters look for the low-hanging fruit. Fraudsters are opting more and more to attack systems en masse, using methods like repeat attempts (we’ll touch more on this later in the report). Fraudsters can produce low-quality, fake documents in the thousands, launch an attack, and hope one slips through a business’s defenses.

That isn’t to say this won’t change — as businesses become more adept at spotting and preventing these types of attacks, fraudsters are bound to adjust their game yet again. This flood of less sophisitcated attacks can also distract from the rarer, but more sophisticated fraud. This is why automating fraud detection to prevent this type of fraud from slipping through is key, so businesses can protect themselves at scale while keeping resources available for potential sophisticated attacks.

> **Fraudsters are choosing quantity over quality —** scalable fraud prevention is a must-have.



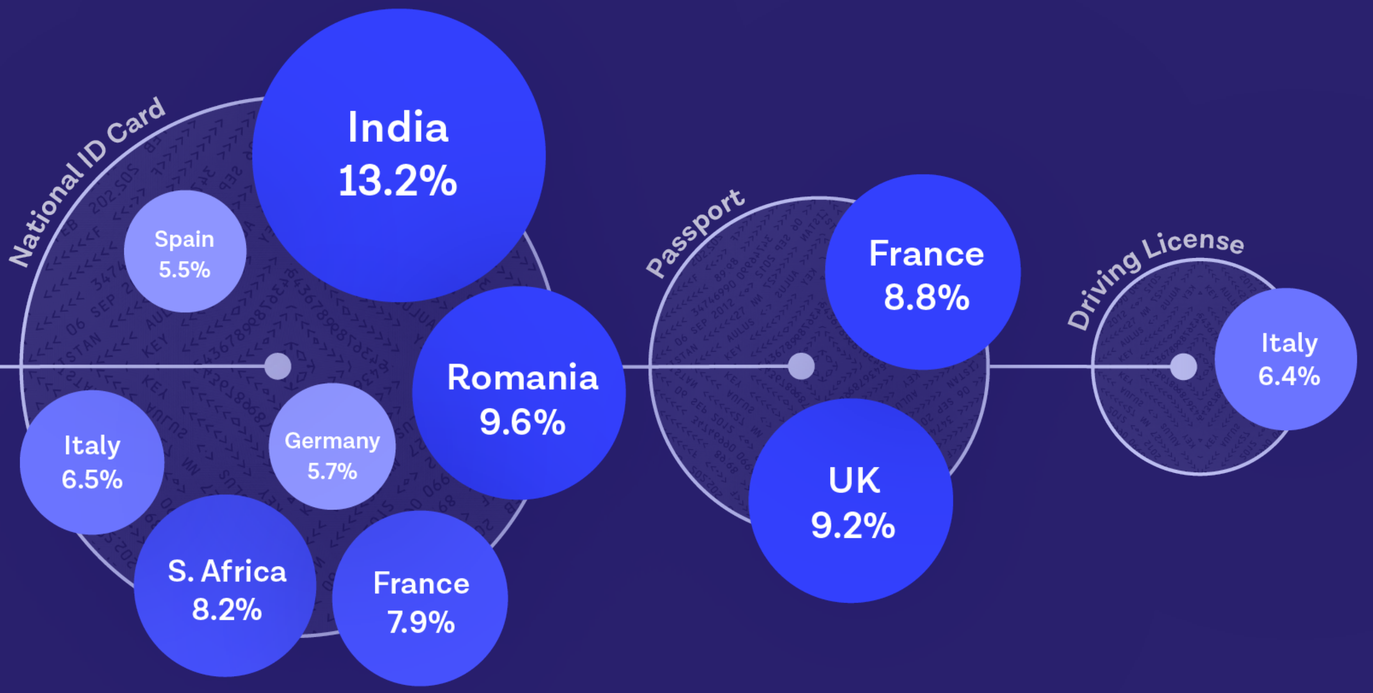
Easy
Document elements are clearly wrong, for example, documents have the wrong font or an obviously attacked photo.

Medium
Less obvious errors, such as less visibly incorrect fonts, the wrong photo printing technique, or imitated security features.

Hard
Cases that require enhanced knowledge of document manufacturing (eg. security features, printing and deliberate mistakes) to detect anomalies.

Top 10 most targeted documents

Suspected fraud (%)



National Identity Card, India	13.2%
National Identity Card, Romania	9.6%
Passport, United Kingdom and Northern Ireland	9.2%
Passport, France	8.8%
National Identity Card, South Africa	8.2%

National Identity Card, France	7.9%
National Identity Card, Italy	6.5%
Driving Licence, Italy	6.4%
National Identity Card, Germany	5.7%
National Identity Card, Spain	5.5%

Fraudsters shift their focus back to National Identity Cards

In 2021 we saw that passports were some of the most targeted documents — six of the top 10 most targeted documents in 2021 were passports.

This year fraudsters have shifted their attention back to National ID Cards. We can see the general focus on National ID Cards in the graph on this page — 46.3% of the suspected fraudulent documents we see are National ID Cards. As a document type, National ID Cards lend themselves to physical counterfeits which is still the type of document fraud we see the most of by far from fraudsters.

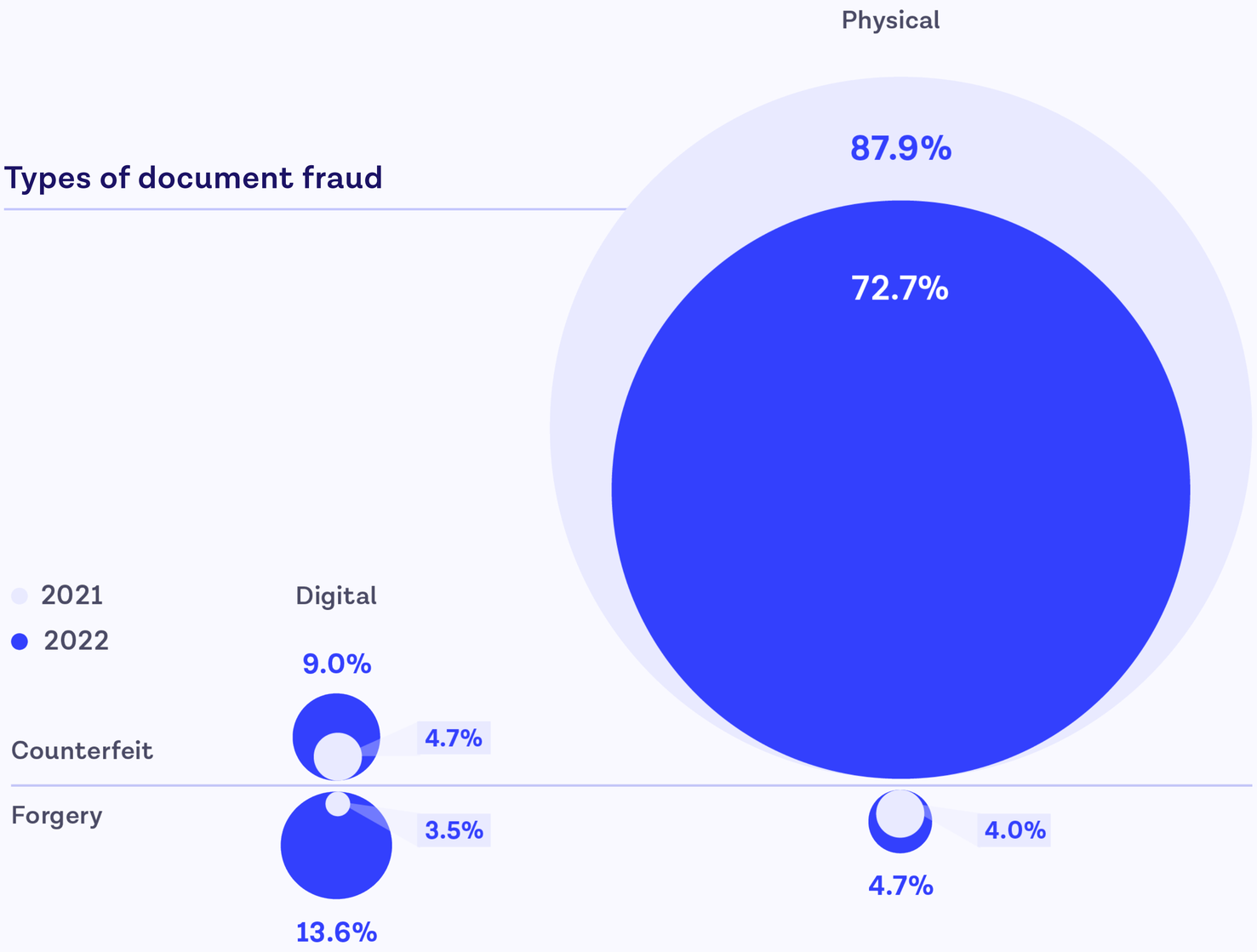
Fraud by document type

Digital forgeries are on the rise

Compared to last year there has been a drop in the number of physical counterfeit documents we're seeing, and a rise in the number of digital forgeries.

This corresponds to the fact that 'easy' fraud has increased. Digital fraud can be easier to spot — for example, some common ways fraudsters attempt to tamper with documents digitally is simply adding their photo on top of the document using photo editing software.

Fraud type	2021	2022
Counterfeit physical	87.9%	**72.7%**
Forgery digital	3.5%	**13.6%**
Forgery physical	4.0%	**4.7%**
Counterfeit digital	4.7%	**9.0%**

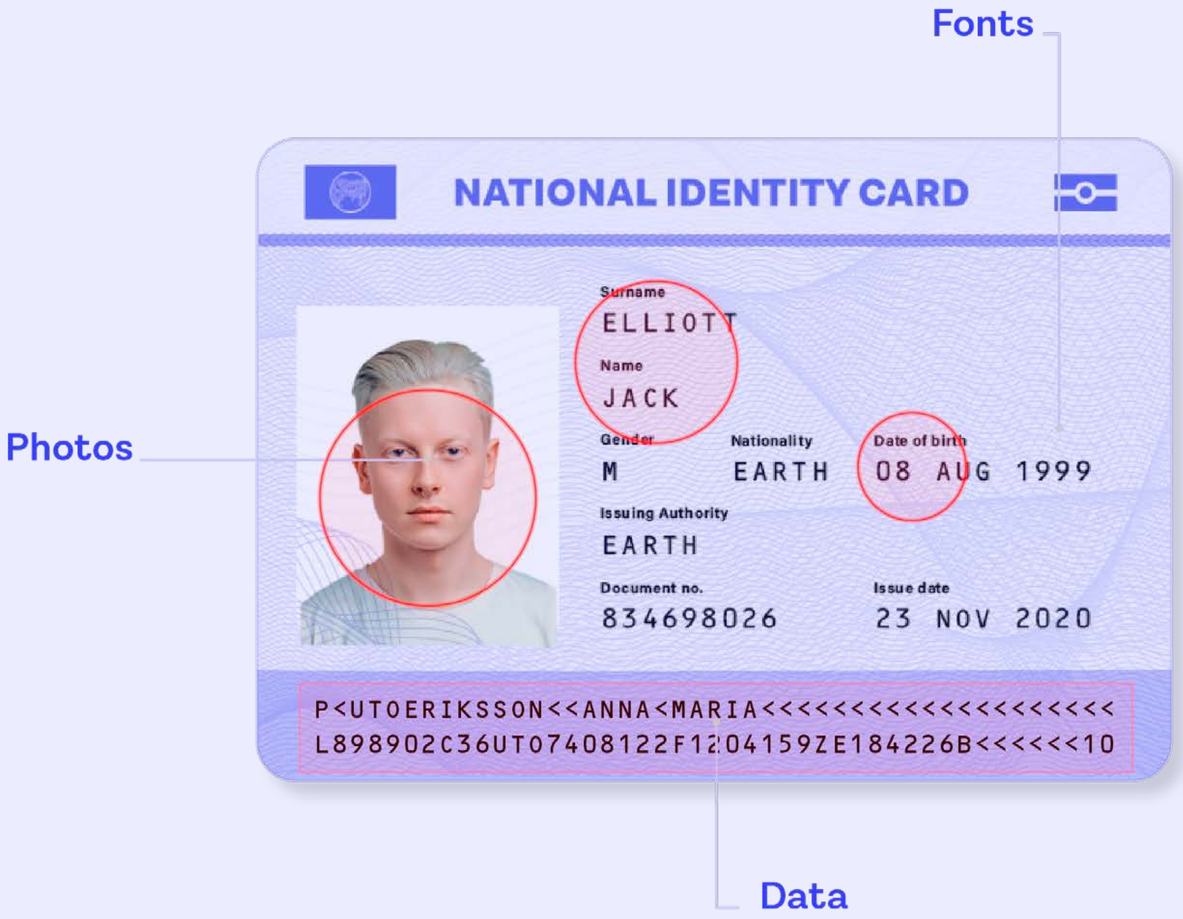


Example of a fraudulent document

This image shows an example of some of the different ways fraudsters commonly target a document.

Some of the most basic signs of fraud to watch out for include:

- **Photos**
  Pictures should be the correct color, or black and white depending on the document type, and the secondary portrait should match the primary picture.
- **Data**
  The information contained in the MRZ (machine readable zone) should reflect the data within the passport
- **Fonts**
  Different documents (and areas of the document) use different types of fonts.



Fraudsters opt for low-effort biometric fraud

Across biometric fraud attempts, overwhelmingly the two types of fraud we see the most are a photo on the screen, where fraudsters capture a photo of an image on a screen as opposed to using their own face, and a spoof of the identity document, where fraudsters present the photo on the document instead of a real face during the biometric step.

This reinforces the fact that fraudsters are opting for less sophisticated fraud, as opposed to more sophisticated attacks like 2D or 3D masks, and that biometric verification remains a great fraud deterrent because of the high hurdle it immediately puts in front of fraudsters.

Photo on screen
A photo or video of an image on screen.

Spoof ID
A photo or video of the image on the identity document.

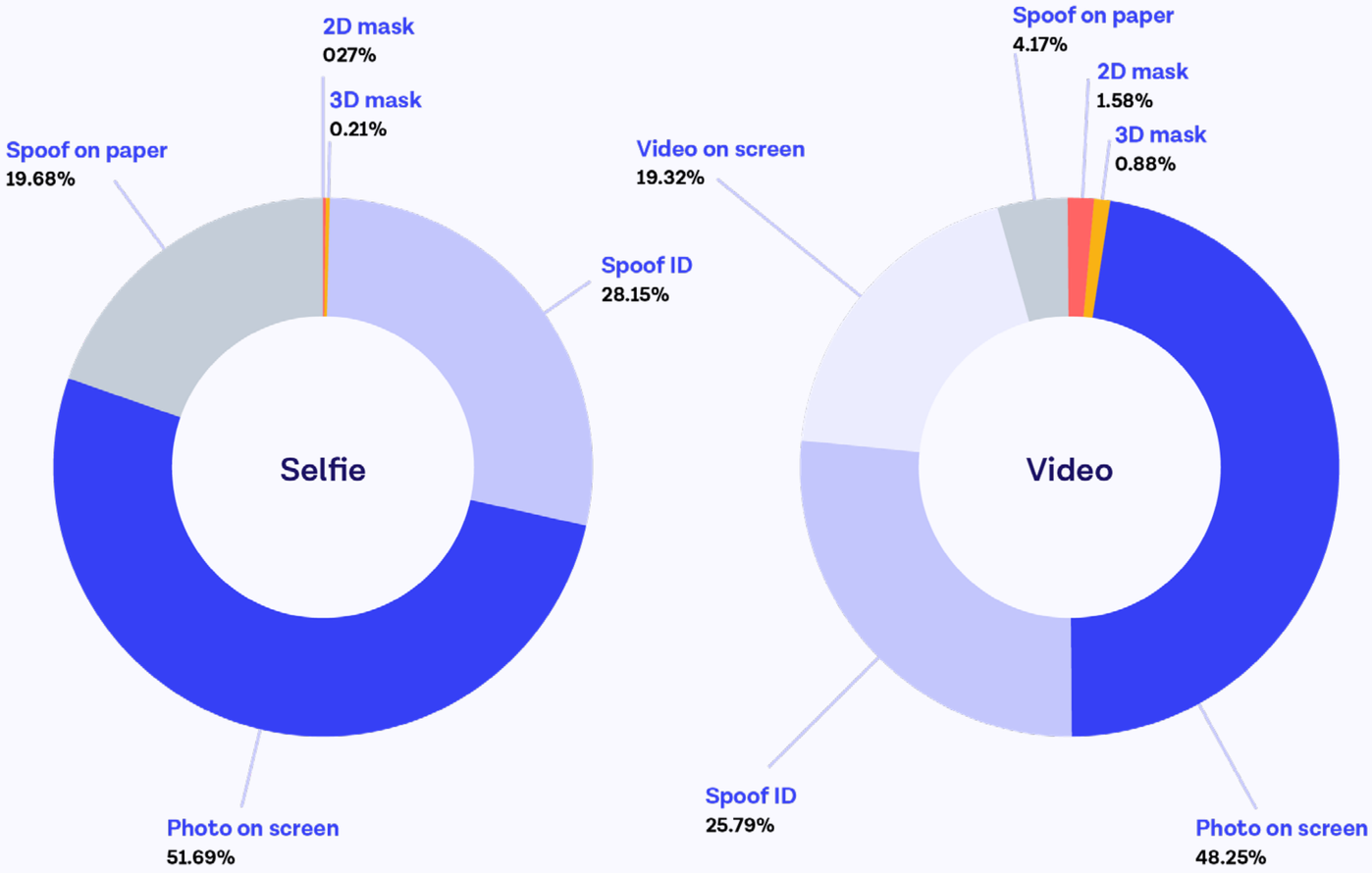
3D mask
A photo or video of a 3D mask or other 3D objects.

Spoof printed on paper
A photo or video of an image printed on paper

2D mask
A photo or video of a 2D printed mask.

Video on screen
(*Video check only*)
A video of a video on screen.

Types of biometric fraud



Device fraud: mapping manufacturers by geography

The list of phone manufacturers that are most commonly flagged for fraud are generally less well-known brands and linked to cheaper phone models.

Fraudsters are likely purchasing cheaper devices to use as burner phones, specifically for the purpose of conducting fraud.

Most fraudulent phone manufacturer by issuing country

We can also see which phone manufacturers are more frequently linked to fraud based on document issuing country.

Businesses can use this information to see where patterns are emerging based on location and phone manufacturer. For example, we can see that TECNO MOBILE, Xaomi and OnePlus crop up several times across multiple countries.

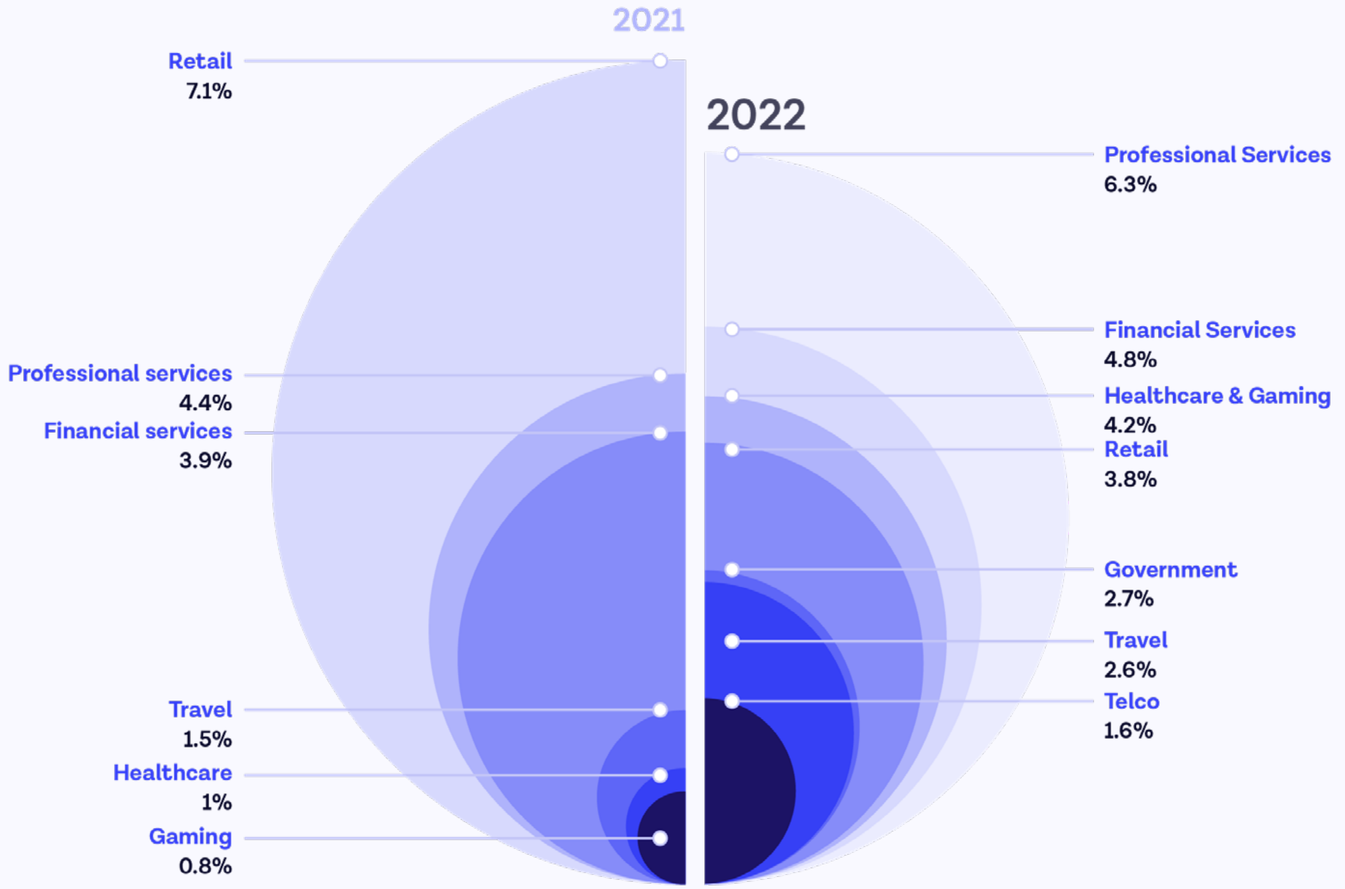
Professional services, financial services and gaming see rise in fraud

In 2021, we saw a big spike in retail fraud. The COVID-19 pandemic forced many brick-and-mortar businesses (including much of the retail industry) to rapidly re-assess online processes which had to be optimized for 100% digital experiences.

As these industries went through this digital transformation, they were an easy target for fraudsters. Fast forward to this year and industries as a whole are better equipped to deal with fraud, which might explain the drop in retail fraud.

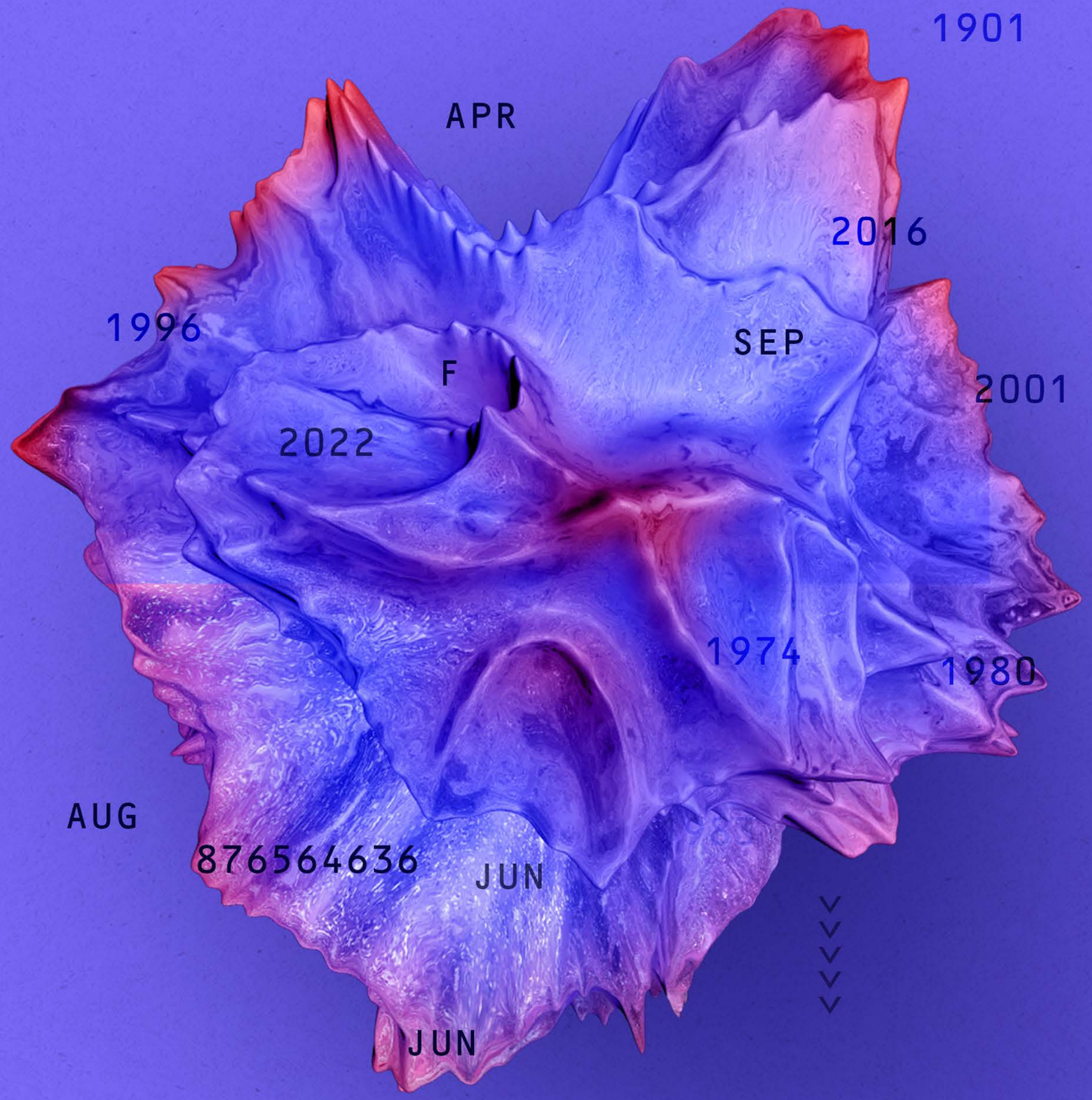
Across other industries, we're generally seeing fraud increase in the areas we would expect. Professional services, financial services, healthcare and gaming have all seen slight increases in fraud. These industries are all well aware of the threat of fraud to their businesses. Priorities should include re-examining onboarding flows to see where they might be vulnerable to emerging fraud threats while reinforcing the processes they already have in place.

Average industry fraud rates



Fraudster techniques

What to expect in 2023



Synthetic identity fraud: unpacking document trends

Synthetic identity fraud is a process where fraudsters combine real and fabricated personal information to create fictitious identities and attempt to benefit from the creation of a fraudulent account or sign-up.

This blending of real and fake information makes the fraud very difficult to detect.

It's also fairly easy for a fraudster to get their hands on real personally identifiable information (PII) data and to create synthetic identities. Data breaches have left huge amounts of data available to buy on the dark web. Atlas VPN found that bundles of data — including Social Security numbers, full names, driver's licensenumbers, passport numbers, and email addresses — are available to buy for as little as $4.

The cost of synthetic identity fraud

$20 billion

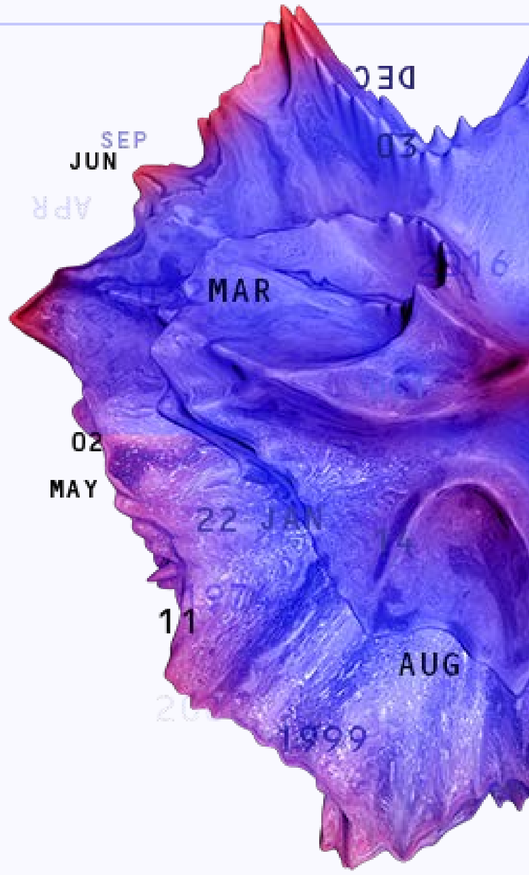
estimated losses of synthetic identity fraud in 2020 (Fiverity)

85%

of all fraud is estimated to be linked to synthetic identity fraud (Federal Trade Commission)

$97,000

the average amount lost to each case of synthetic identity fraud (PYMNTS)



According to the Federal Reserve, “**the ease of synthetic creation, combined with the increase in digital account applications capabilities, have simplified the process of creating these fictitious people**” and they are “often undetected by traditional fraud models” since these models “are not built around the idea that a person is not real.”

We see fraudsters mostly tar-geting documents when it comes to synthetic identity fraud.

This is because it requires less input from a fraudster's perspective — all they need to do is tweak a few pieces of information on the document. Some of the areas of the document we routinely see fraudsters target are:

- **Name**
- **Date of birth**
- **Document number**
- **Photo**

Document data

Gender

There are some signs that businesses can look for to help identify synthetic identity fraud across documents. For one thing, our data shows that fraudsters are 37% more likely to create documents using a 'male' classification on documents that include gender as part of the document data.

Gender	Suspected %
Male	5.19%
Female	3.79%

First name, surname

We're also seeing fraudsters leveraging fictional names across documents.

For example, one of the names that was frequently flagged for fraud this year was (first name) EDWARD (last name) CULLEN (for anyone who isn't aware, a character from a fictional novel series.). It appears that fraudsters lean towards using specimen or sample documents when using fake PII, and opt for last names like SPECIMEN, NULL or SAMPLE.

Genuine document

Real and slightly altered PII

Real and fake PII (data)

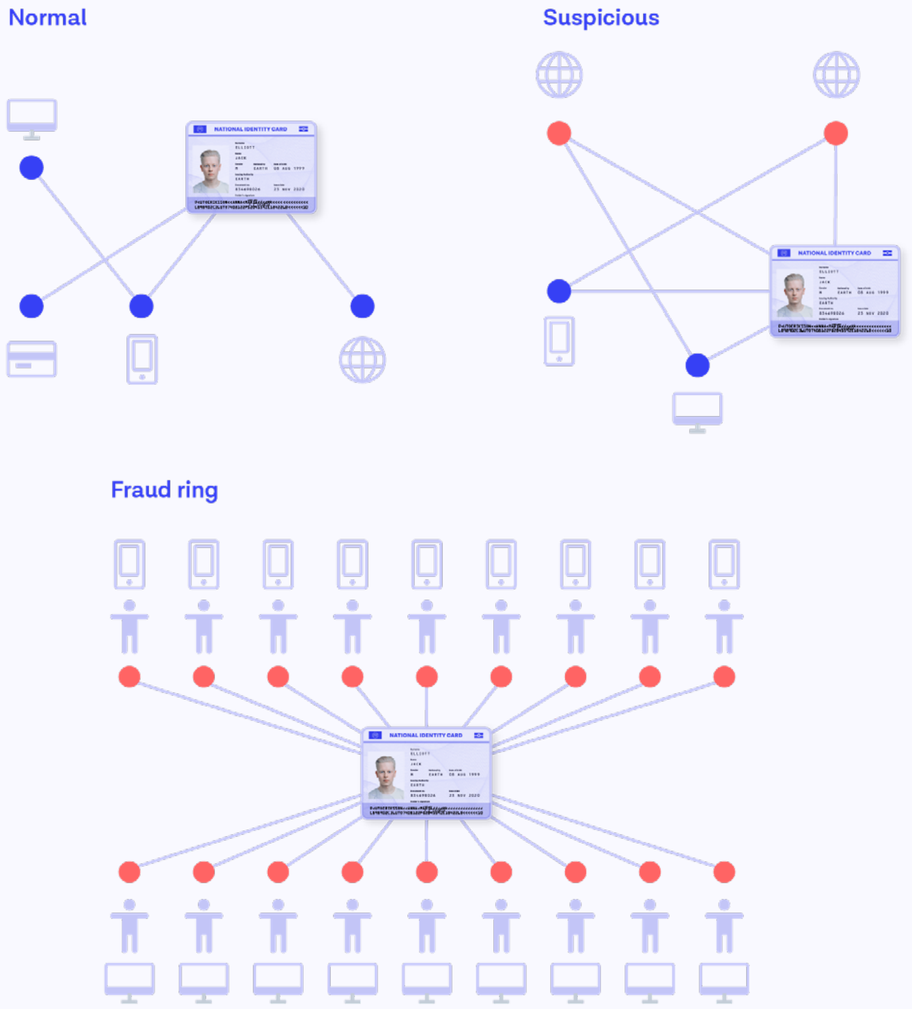
Real and fake PII (photo)

Identifying fraud rings through repeat attempts

Different types of fraud can have varying degrees of impact on businesses. Something that many businesses are rightfully concerned about is organized attacks linked to fraud rings.

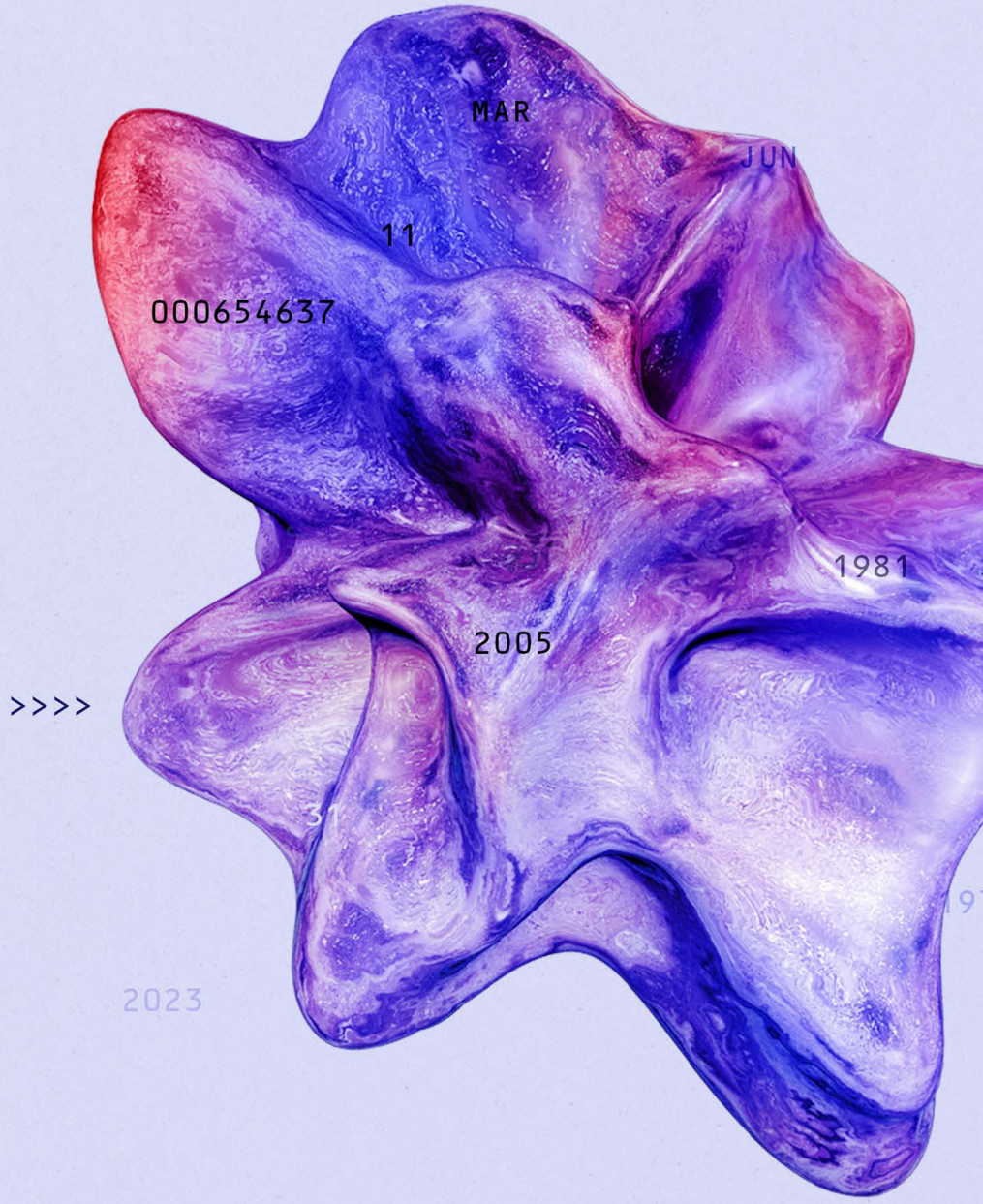
Identifying fraud rings is increasingly difficult given the myriad of tools and methods fraudsters can access to subvert systems and launch coordinated, organized attacks.

But one major indicator of a possible fraud ring that businesses can watch for is instances of repeat fraud. Criminals use the same or similar information over and over to launch large-scale attacks. Criminals make hundreds, if not thousands, of copies of the same document, but tweak minor details each time. For example, the documents might all have the same face and personal information, with the exception of the document number which changes by one number each time. Or vice versa, the document numbers might all be the same, but the name on the document varies each time.



One piece of information fraudsters commonly repeat across documents is the document number.

In such scenarios, fraudsters launch an attack by submitting the same document type with the same unaltered document number, hundreds if not thousands of times.



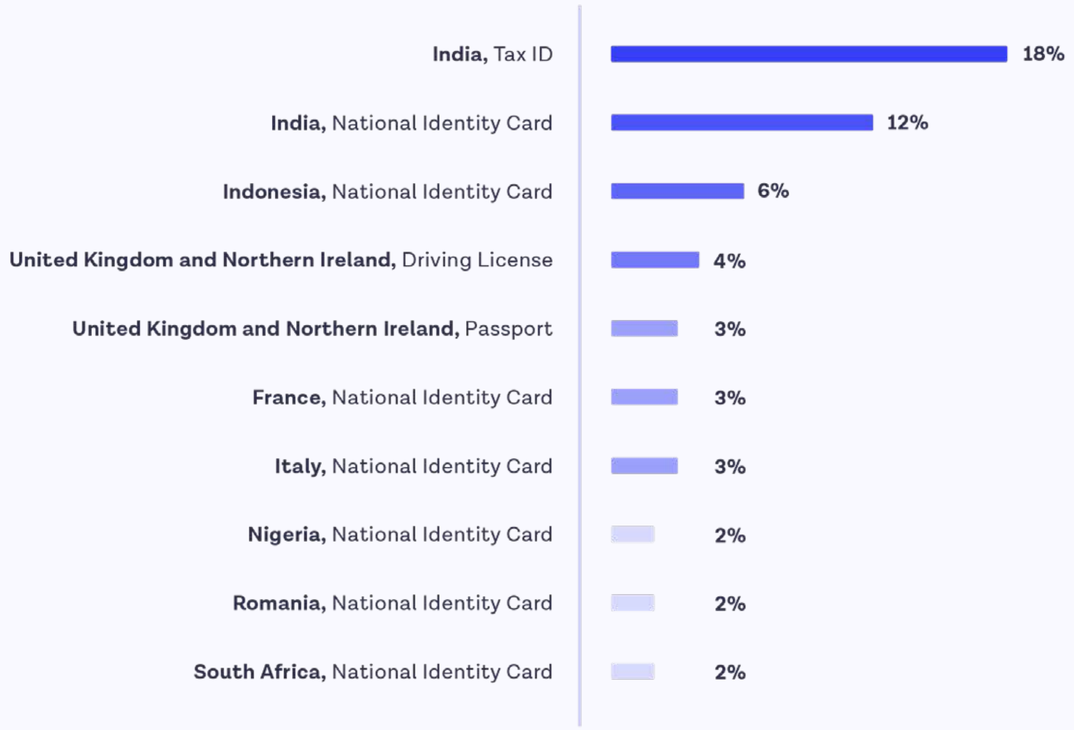
Preventing repeat fraud by analyzing document numbers

One piece of information fraudsters commonly repeat across documents is the document number.

In such scenarios, fraudsters launch an attack by submitting the same document type with the same unaltered document number, hundreds if not thousands of times.

Here we can see which documents fraudsters most frequently use during repeat attacks — the data shows how often a document gets flagged for fraud because we've identified the same document number across that document type. Based on this data, businesses would be able to stop 18% of fraud attacks coming from the India Tax ID just by looking at the document number alone. This is where Onfido's Repeat Attempts can help businesses prevent huge amounts of fraud by automatically identifying repeat information.

Documents with repeat document numbers



Client stories: Repeat Attempts in action

Client 1

95 fraud rings identified

In three months. *With the help of repeat attempts, this client identified that the same document number was submitted* **300 times** *combined with different attributes.*

Client 2

60 fraud rings uncovered

In this case, the client found that **20 fraud rings** *had submitted the same documents more than* **100 times.**

Client 3

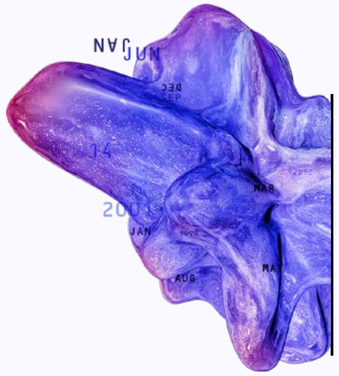
17,052 instances

Where the same document was submitted multiple times, identified with the help of repeat attempts.
Of these documents there were three separate instances where **the exact same document was used 50+ times**

Document 1 → *submitted* **104 times**

Document 2 → *submitted* **71 times**

Document 3 → *submitted* **55 times**



Repeat Attempts is Onfido's solution to catching repeat fraud. It operates in the background when a user undergoes Document Verification, comparing document data to historic onboarded documents to detect repeat ID document usage.

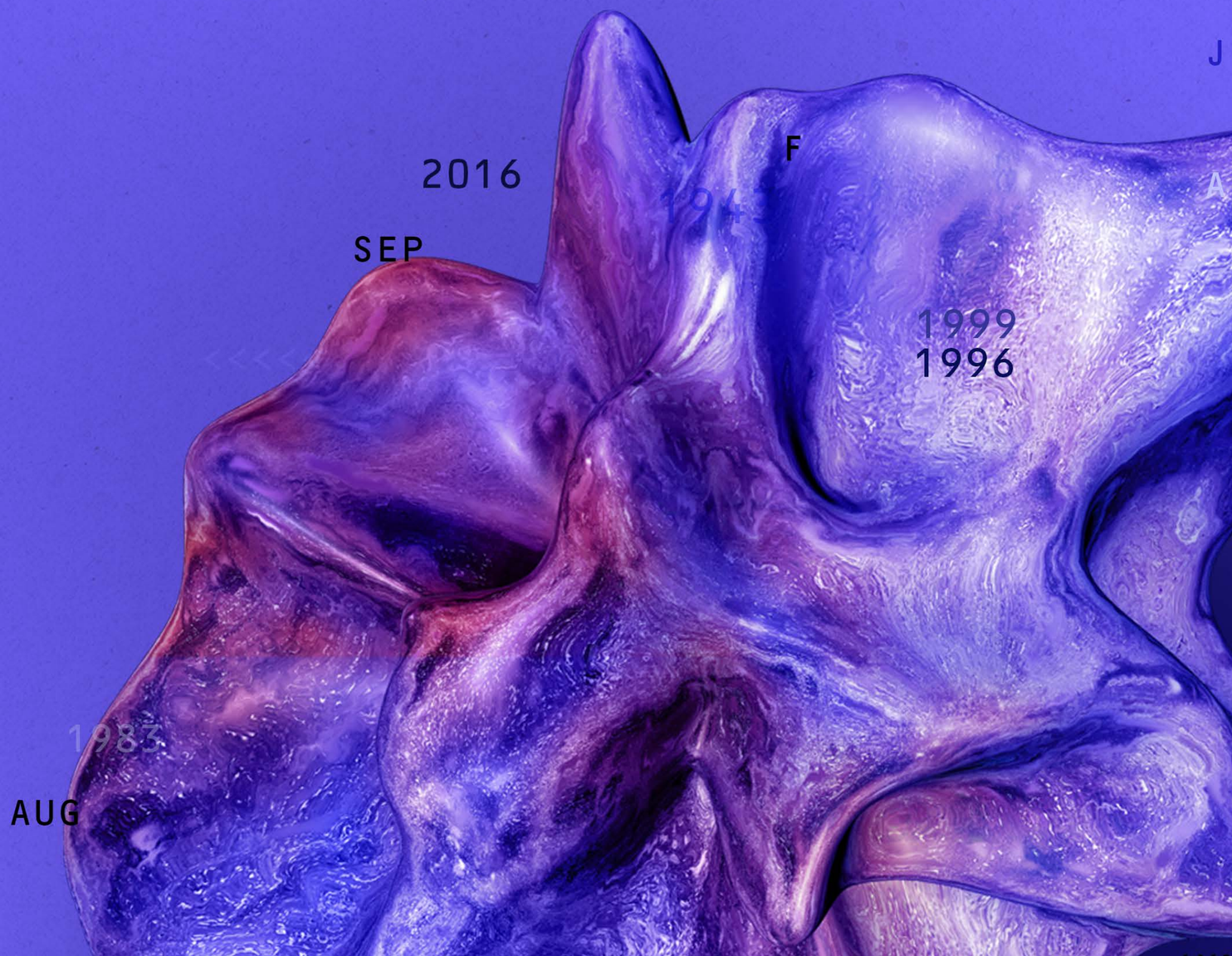
Pre-empting bonus abuse fraud

It's well known that fraudsters follow the money. This includes promotional sign-ups and cash bonus campaigns.

Across our clients, we've seen that fraud rates tend to spike when onboarding numbers increase (as fraudsters like to hide among the volume) for example when a business launches a sign-up campaign. This includes when banking or gaming companies offer a sign-up or referral bonus, or a crypto company drops a new coin listing.

For businesses that are about to launch a campaign, let identity providers know about it upfront. Protecting against fraud is a two-way process, and forewarning providers in advance means they can help businesses prepare for spikes in volume to get the best coverage.

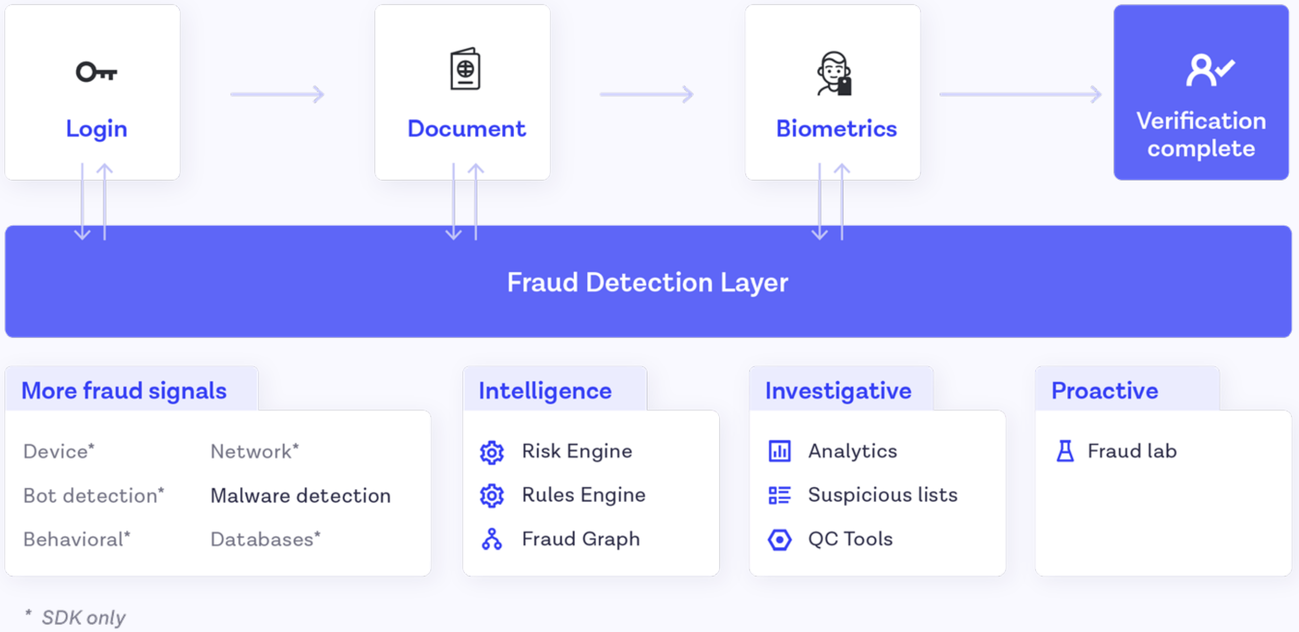
Prevention best practice



1. Make onboarding your business stronghold

A strong fraud defense starts early. Onboarding is the first touch point any business has with a customer, and this is where fraud detection should start.

As Interpol noted in their foreword, identity fraud is closely linked to money laundering and other financial crime. If businesses leave themselves vulnerable to fraud at onboarding, they risk opening themselves up to such activities, which can have a knock-on effect on compliance.



2. Adopt a layered approach

There is no one-size-fits-all approach to detecting and preventing fraud.

Fraudsters are always going to look for new ways to get around defenses — and as soon as they find an avenue to exploit they'll throw everything at it. Relying on one form of verification alone can leave businesses vulnerable.

This is why it's so important to leverage a multi-layered approach to fraud detection.

The threat of synthetic identity fraud also highlights the importance of adopting a layered approach. The availability of fake and real PII due to data breaches, and the many different ways fraudsters can manipulate this data, means one fraud detection method alone is never going to catch it. But layering intelligence from devices, networks, locations and identities with verification checks that validate credentials like SSN with the source of truth will give businesses a much better chance at weeding out fraud. The diagram shows what this might look like in practice.

3. Use SDK over API

At Onfido we provide a set of SDKs for our customers to integrate an optimized, accessible document and face capture flow into their own apps.

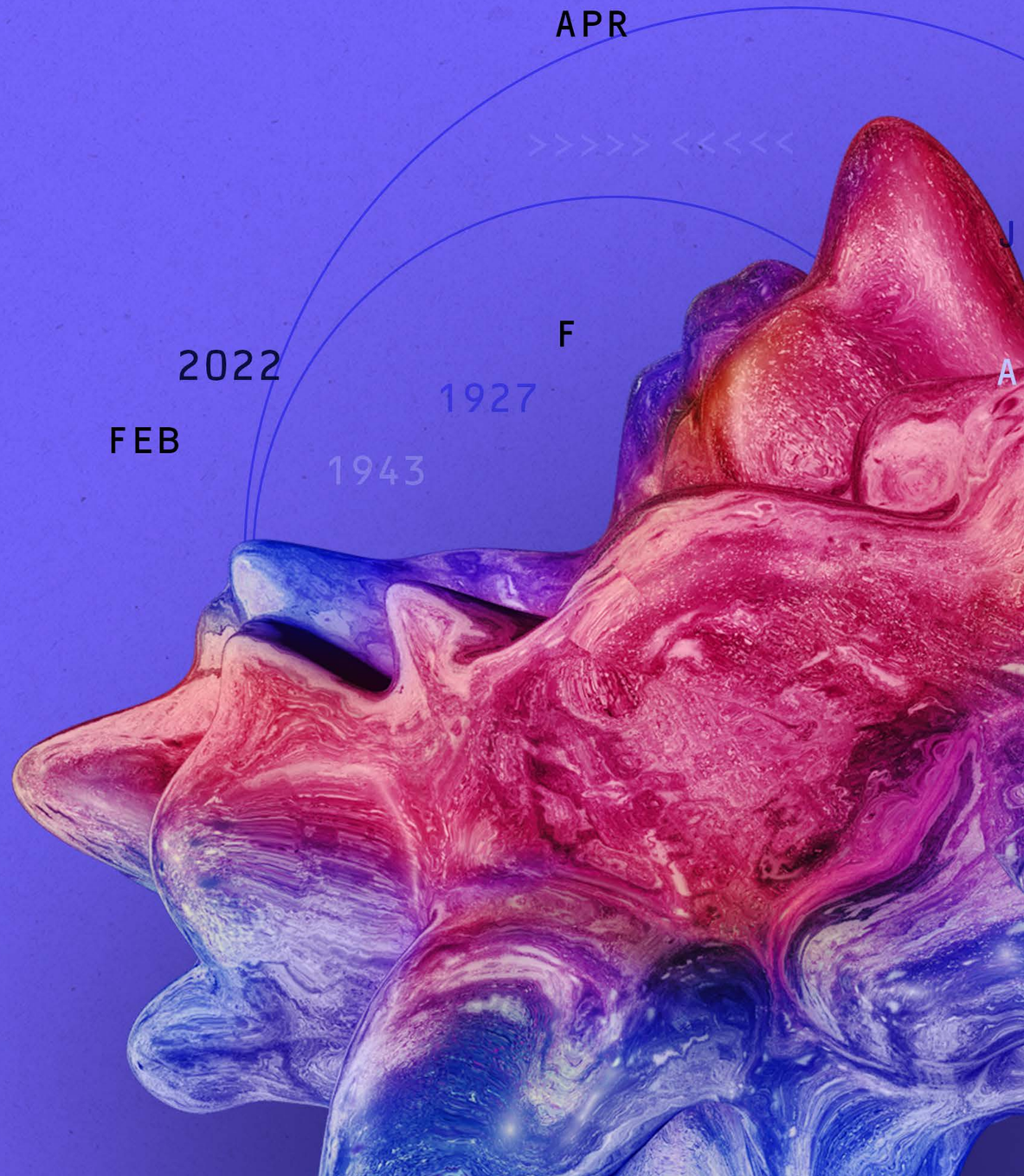
Alternatively, the Onfido API enables clients to submit verification checks programmatically. The SDKs offer several benefits and give businesses more control from start to finish. Using the SDKs means easier and more flexible integration, more consistent image quality, accessible UX, and better fraud deterrence. We see fewer suspected fraudulent cases via our SDKs because live capture greatly reduces the chance of digitally tampered image submission, while our device integrity checks ensure the authenticity of captures.

4. Leverage automation

As we've seen throughout this report, fraudsters are opting for quantity over quality and attacking businesses en masse. Therefore it's vital that businesses are able to ramp up fraud defenses and protect themselves at scale. This is where automation comes in.

Fraud detection solutions that use algorithms trained on both fraudulent and genuine datasets are preferable. They are more accurate at detecting documents and individuals who might require further investigation. Plus they detect fraud in real-time, speeding up the process where manual reviews might leave genuine customers waiting. AI-driven fraud detection is also more cost effective. Freeing up internal teams by removing the need for them to perform manual reviews means their time can be spent on other, more complex tasks that require human intervention.

Onfido’s approach to fraud detection



Verification Suite

Four layers of fraud detection

Document verification

End users take a photo of their identity document and Onfido checks for fraud.

Onfido's Atlas™ AI checks the data on documents is valid and consistent, that the image isn't a scan, photo of a screen, print out or screenshot, and examines the picture, font, shape/layout, and security features to determine authenticity.

+ Repeat Attempts:
Identify duplicate information to protect against documents that include the same information.

Biometric verification

End users take a selfie or turn their head (Motion), and Onfido compares the photo on the ID to their biometrics.

We return a similarity score based on whether the biometric matches what is on the submitted ID and also perform spoof detection, checking for masks, pictures of a printout, videos of a video, or repetition of document photos.

+ Known Faces:
Identify repeat fraudsters and know when a duplicate face has entered the system.

Data verification

Validate customer identities against a range of trusted data sources, including

- **SSN:** Electronically verify US Social Security numbers
- **ID Record:** Access databases in over 160 countries, including voter registers, consumer, credit, and utility databases
- **Watchlist and ongoing monitoring:** Sanctions lists, adverse media categories, and PEPs
- **Proof of address:** Automated PoA document verification.

Fraud detection signals

Create a 360-degree view of customer identities with a range of passive fraud signals, including:

- **Device data:** Integrity of the device and app, operating system, image metadata
- **Network data:** Device network information including IP reputation, geo locators, use of VPN
- **Behavioral data:** User interaction within the app, database checks

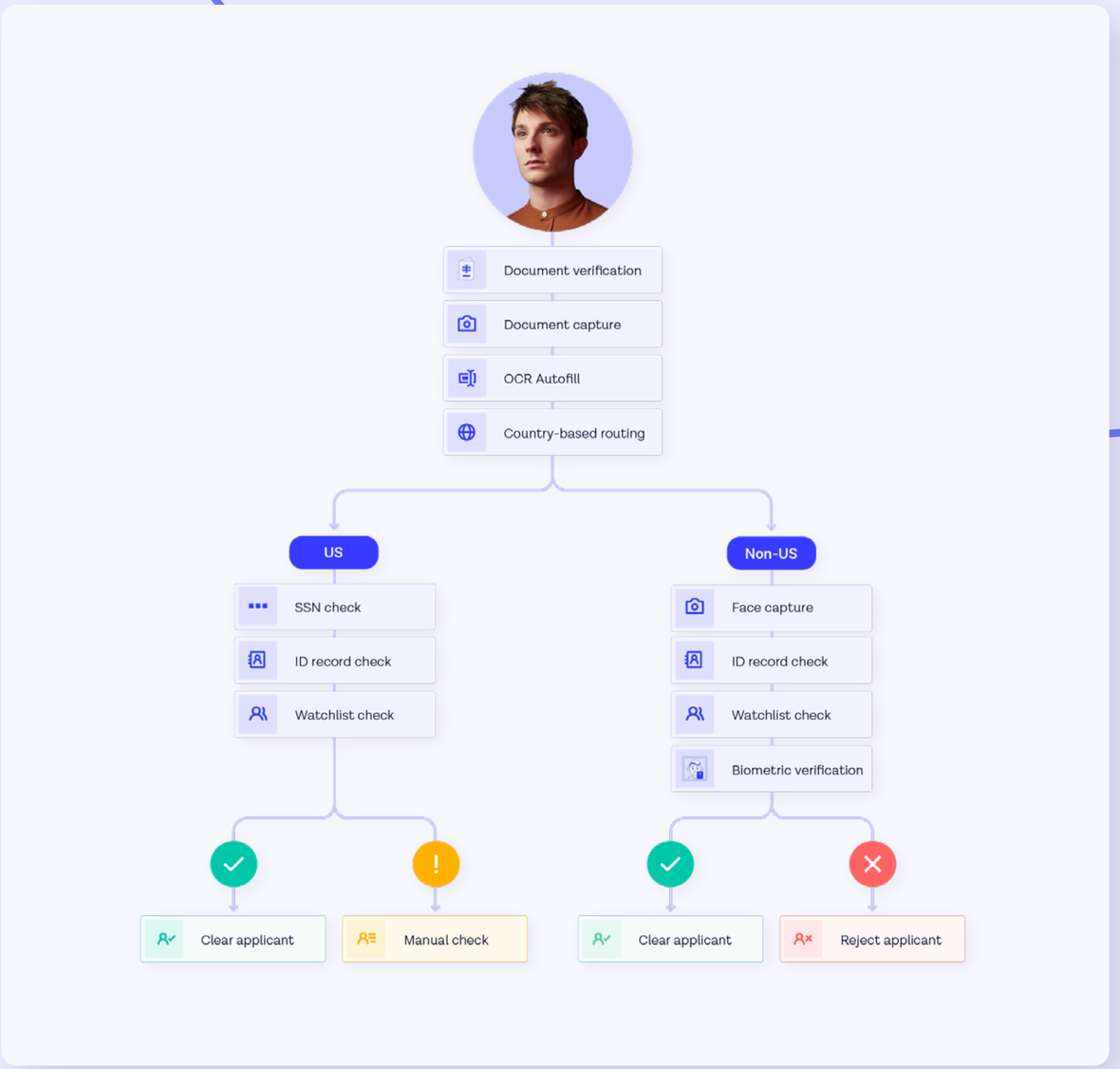
Onfido Studio

Orchestrating onboarding flows for fraud prevention

Onfido Studio is mission control for building out onboarding flows.

It's how businesses orchestrate verification journeys that combine document and biometric verification, data sources, and fraud detection signals.

Studio is all about agility. Drag-and-drop workflows mean businesses can quickly react to changes they're seeing in market, tailoring verification journeys to combat specific fraud vectors in real time.

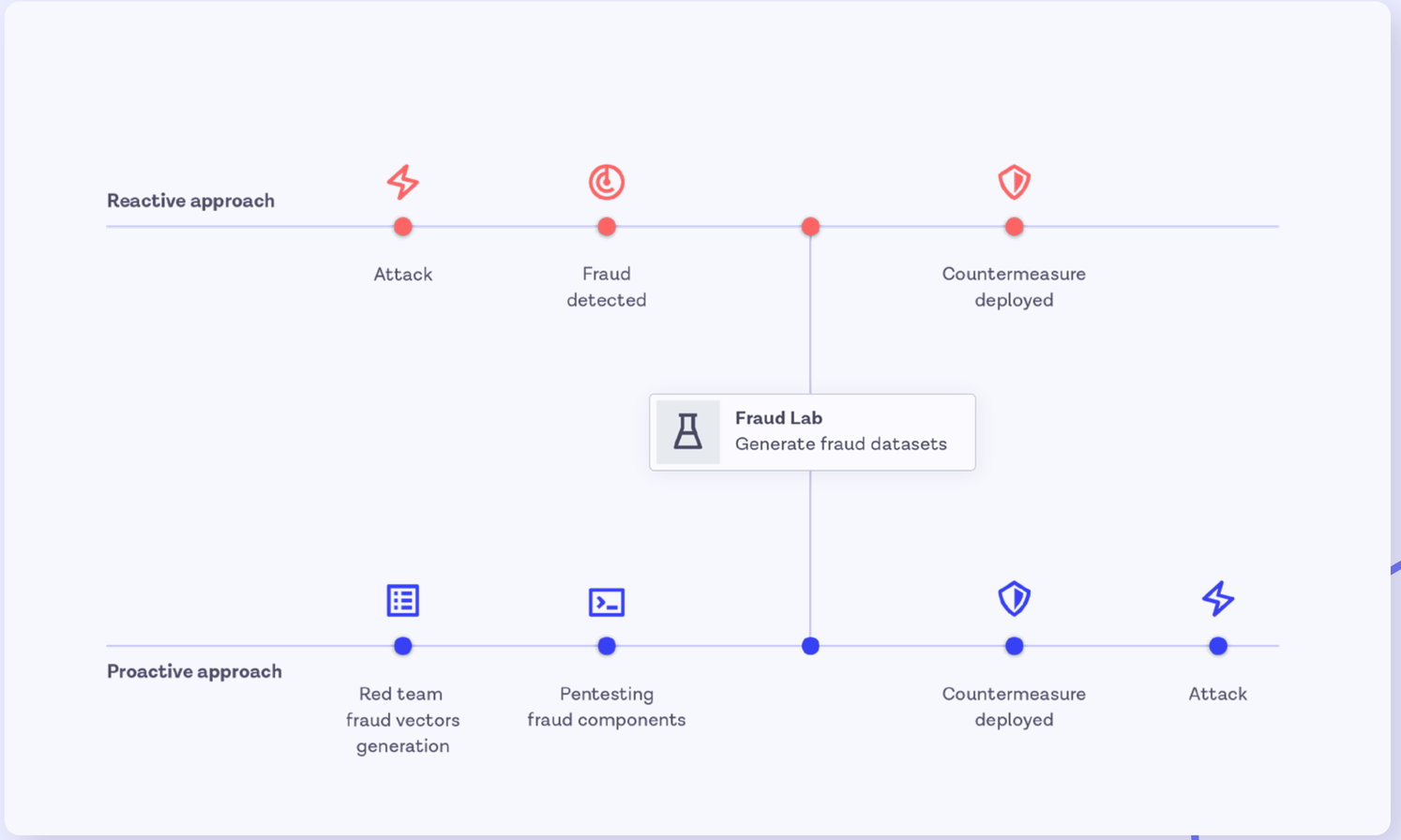


Onfido Fraud Lab

A proactive approach to fraud prevention

A reactive approach to fraud leaves businesses vulnerable to reputational damage and monetary losses, not to mention forever playing catch up with the fraudsters.

Onfido Fraud Labs is our solution to this — the best defense is a good offense. A team of Onfido experts is dedicated to replicating fraud in-house using both physical and digital spoofs. We're then using these fraudulent datasets to train our algorithms, so they're better at detecting both genuine and fraudulent attacks.



Closing statement

“When we compare 2022 to the previous two years, much of the world has returned to ‘business as usual’ following the outbreak of COVID-19.

This return to relative normalcy has seen fraud rates drop slightly. The higher fraud rates we saw in 2020 and 2021 were directly tied to the COVID pandemic — turbulence always creates opportunity for fraud, and increased digital activity as a result of the pandemic created plenty of opportunity.

But as a result, we’re likely to see some long-term fallout on fraudulent activity. For one thing, the interconnectedness of global business and the immediacy digital access provides means fraud now happens from anywhere in the world, at any time. It’s a 24/7 business. With fraudsters taking an increasingly holistic approach, it’s vital businesses do the same in their approach to prevention.

Here are a few things to consider:

- The best defense is a layered one — don’t rely on one approach alone to catch fraud
- We still see the benefits of combining document and biometrics, the latter providing a higher bar for fraudsters to bypass
- Passive signals (such as device, network and location intelligence) add further protection, without adding friction for genuine customers
- Some solutions might be simple but they can be incredibly effective, for example, repeat attribute detection

Looking to the future, I think we can expect to see NFC playing a much larger role in identity verification. NFC verification is incredibly fast, accurate and adds another layer of security. Deepfakes are also on the horizon, and while we can’t know when exactly they might become mainstream (today they are still a rare occurrence) the technology is out there, so be sure to have liveness detection in place. Digital and virtual identity documents, and the opportunities they create for reusable identity, are also on the rise. It’s a space to watch — one that could open up huge opportunities, but also new avenues for fraud.”

Simon Horswell

Fraud Expert, Onfido

An experienced expert in ID security and fraud, Simon plays a key role in Onfido’s product development strategy. Prior to Onfido, Simon served as an Expert Document Examiner and trainer for several years at the UK’s National Document Fraud Unit (NDFU), and subsequently worked as a Document Expert and international trainer with Foster & Freeman Ltd.

Contributors

Fraud experts

SIMON>>>>
HORSEWELL
Fraud Specialist

MICHAEL>>>
VAN>GESTEL
VP of Expert Services

ELLIE>BURNS
Senior Product
Marketing Manager

VINCENT>>
GUILLEVIC
Director of Fraud Labs

Data scientists

DOGUCAN>
BASKIN>>
Product Operations
Manager

VIRGINIA>>
CHIARENTIN
Product Operations
Analyst